Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes

Ryutaroh Matsumoto
ryutaroh@ss.titech.ac.jp
Tomohiko Uyematsu
uematsu@ss.titech.ac.jp
Dept. of Electrical & Electronic Eng.,
Tokyo Instutute of Technology,
2-12-1 Ookayama, Meguro-ku, Tokyo, 152-8552 Japan

November 4, 1999

Abstract

We generalize the construction of quantum error-correcting codes from $\mathbf{F}_4$-linear codes by Calderbank et al. to p^m-state systems. Then we show how to determine the error from a syndrome.

1 Introduction

Quantum-error correcting codes have been paid much attention. Among many research articles, most general and systematic construction is the so called *stabilizer code construction* [4] or *additive code construction* [1], which construct a quantum error-correcting code as an eigenspace of an Abelian subgroup S of the error group. Then Calderbank et al. [2] proposed a construction of S from an additive code over the finite field $\mathbf{F}_4$ with 4 elements.

These constructions work for tensor products of 2-state quantum systems. But Knill [5, 6] and Rains [8] observed that the construction [1, 4] can be generalized to n-state systems by appropriate choice of the error basis. We propose a construction of quantum error-correcting codes for p^m-state systems from classical error-correcting codes which is a generalization of [2]. Throughout this note, p denotes a prime number and m a positive integer.

2 Stabilizer coding for p^m-state systems

We review the generalization [5, 6, 8] of the construction [1, 4]. First we consider p-state systems. Let λ be a primitive p-th root of unity, C_p, D_λ $p \times p$ matrices defined by $(C_p)_{ij} = \delta_{j,i+1 \bmod p}$, $(D_\lambda)_{ij} = \lambda^i \delta_{i,j}$. We shall construct a quantum

code encoding quantum information in p^k-dimensional linear space into $\mathbb{C}^{p^n}$. We consider the error group consisting of $\lambda^j w_1 \otimes \cdots \otimes w_n$, where j is an integer, w_i is $C_p^a D_\lambda^b$ with some integers a, b.

For vectors $(\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}') \in \mathbf{F}_p^{2n}$, we define the alternating inner product

$$((\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}')) = \langle \boldsymbol{a}, \boldsymbol{b}' \rangle - \langle \boldsymbol{a}', \boldsymbol{b} \rangle, \tag{1}$$

where $\langle , \rangle$ denotes the standard inner product in $\mathbf{F}_p^n$. For $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbf{F}_p^n$, we define

$$\begin{aligned} X(\boldsymbol{a}) &= C_p^{a_1} \otimes \cdots \otimes C_p^{a_n}, \\ Z(\boldsymbol{a}) &= D_\lambda^{a_1} \otimes \cdots \otimes D_\lambda^{a_n}. \end{aligned}$$

Then we have

$$X(\boldsymbol{a})Z(\boldsymbol{b})X(\boldsymbol{a}')Z(\boldsymbol{b}') = \lambda^{\langle \boldsymbol{a}, \boldsymbol{b}' \rangle - \langle \boldsymbol{a}', \boldsymbol{b} \rangle} X(\boldsymbol{a}')Z(\boldsymbol{b}')X(\boldsymbol{a})Z(\boldsymbol{b}). \tag{2}$$

For $(\boldsymbol{a}|\boldsymbol{b}) = (a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathbf{F}_p^{2n}$, we define the weight of $(\boldsymbol{a}|\boldsymbol{b})$ to be

$$\sharp\{i \mid a_i \neq 0 \text{ or } b_i \neq 0\}. \tag{3}$$

Theorem 1 *Let C be an $(n-k)$-dimensional $\mathbf{F}_p$-linear subspace of $\mathbf{F}_p^{2n}$ with the basis $\{(\boldsymbol{a}_1|\boldsymbol{b}_1), \ldots, (\boldsymbol{a}_{n-k}|\boldsymbol{b}_{n-k})\}$, $C^\perp$ the dual space of C with respect to the inner product (1). Suppose that $C \subseteq C^\perp$ and the minimum weight (3) of $C^\perp \setminus C$ is d. Then the subgroup S of E generated by $\{X(\boldsymbol{a}_1)Z(\boldsymbol{b}_1), \ldots, X(\boldsymbol{a}_{n-k})Z(\boldsymbol{b}_{n-k})\}$ is Abelian, and an eigenspace of S is an $[[n, k, d]]_p$ quantum code.*

Next we consider quantum codes for p^m-state systems, where m is a positive integer. But the code construction for p^m-state systems is almost the same as that for p-state systems, because the state space of a p^m-state system can be regarded as the m-fold tensor products of that of a p-state system. We shall construct a quantum code encoding quantum information in p^{mk}-dimensional linear space into $\mathbb{C}^{p^{mn}}$. For $(\boldsymbol{a}|\boldsymbol{b}) = (a_{1,1}, a_{1,2}, \ldots, a_{1,m}, a_{2,1}, \ldots, a_{n,m}, b_{1,1}, \ldots, b_{n,m}) \in \mathbf{F}_p^{2mn}$, we define the weight of $(\boldsymbol{a}|\boldsymbol{b})$ to be

$$\sharp\{i \mid \text{there exists nonzero element in } \{a_{i,1}, \ldots, a_{i,m}, b_{i,1}, \ldots, b_{i,m}\}\}. \tag{4}$$

Corollary 2 *Let C be an $(mn - mk)$-dimensional $\mathbf{F}_p$-linear subspace of $\mathbf{F}_p^{2mn}$ with the basis $\{(\boldsymbol{a}_1|\boldsymbol{b}_1), \ldots, (\boldsymbol{a}_{mn-mk}|\boldsymbol{b}_{mn-mk})\}$, $C^\perp$ the dual space of C with respect to the inner product (1). Suppose that $C \subseteq C^\perp$ and the minimum weight (4) of $C^\perp \setminus C$ is d. Then the subgroup S of E generated by $\{X(\boldsymbol{a}_1)Z(\boldsymbol{b}_1), \ldots, X(\boldsymbol{a}_{mn-mk})Z(\boldsymbol{b}_{mn-mk})\}$ is Abelian, and an eigenspace of S is an $[[n, k, d]]_{p^m}$ quantum code.*

3 Construction of quantum codes for p-state systems from classical codes

3.1 Codes for p-state systems

In this subsection we describe how to construct quantum codes for p-state systems from additive codes over $\mathbf{F}_{p^2}$. Let ω be a primitive element in $\mathbf{F}_{p^2}$.

Lemma 3 *$\{\omega, \omega^p\}$ is a basis of $\mathbf{F}_{p^2}$ over $\mathbf{F}_p$.*

Proof. When $p = 2$ the assertion is obvious. We assume that $p \geq 3$. Suppose that $\omega^p = a\omega$ for some $a \in \mathbf{F}_p$. Then $\omega = \omega^{p^2} = (a\omega)^p = a^2\omega$, and a is either 1 or -1. If $a = 1$, then $\omega \in \mathbf{F}_p$ and ω is not a primitive element. If $a = -1$, then $\omega^{2p} = \omega^2$. This is a contradiction, because ω is a primitive element and $2p \not\equiv 2 \pmod{p^2 - 1}$. ∎

For $(\boldsymbol{a}|\boldsymbol{b}) \in \mathbf{F}_p^{2n}$ we define $\phi(\boldsymbol{a}|\boldsymbol{b}) = \omega\boldsymbol{a} + \omega^p\boldsymbol{b}$. Then the weight (3) of $(\boldsymbol{a}|\boldsymbol{b})$ is equal to the Hamming weight of $\phi(\boldsymbol{a}|\boldsymbol{b})$. For $\boldsymbol{a} = (a_1, \ldots, a_n), \boldsymbol{b} \in \mathbf{F}_{p^2}^n$, we define the inner product of $\boldsymbol{a}$ and $\boldsymbol{b}$ by

$$\langle \boldsymbol{a}, \boldsymbol{b}^p \rangle - \langle \boldsymbol{a}^p, \boldsymbol{b} \rangle = \langle \boldsymbol{a}, \boldsymbol{b}^p \rangle - \langle \boldsymbol{a}, \boldsymbol{b}^p \rangle^p \tag{5}$$

where $\langle , \rangle$ denotes the standard inner product in $\mathbf{F}_{p^2}^n$ and $\boldsymbol{a}^p = (a_1^p, \ldots, a_n^p)$. For $(\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}') \in \mathbf{F}_p^{2n}$ the inner product (5) of $\phi(\boldsymbol{a}|\boldsymbol{b})$ and $\phi(\boldsymbol{a}'|\boldsymbol{b}')$ is

$$\begin{aligned} & \langle \phi(\boldsymbol{a}|\boldsymbol{b}), \phi(\boldsymbol{a}'|\boldsymbol{b}')^p \rangle - \langle \phi(\boldsymbol{a}|\boldsymbol{b})^p, \phi(\boldsymbol{a}'|\boldsymbol{b}') \rangle \\ = \; & \langle \omega\boldsymbol{a} + \omega^p\boldsymbol{b}, \omega^p\boldsymbol{a}'^p + \omega\boldsymbol{b}'^p \rangle - \langle \omega^p\boldsymbol{a}^p + \omega\boldsymbol{b}^p, \omega\boldsymbol{a}' + \omega^p\boldsymbol{b}' \rangle \\ = \; & (\omega^2 - \omega^{2p})(\langle \boldsymbol{a}, \boldsymbol{b}' \rangle - \langle \boldsymbol{a}', \boldsymbol{b} \rangle). \end{aligned}$$

Since ω is a primitive element, $\omega^2 \neq \omega^{2p}$. Thus the inner product (1) of $(\boldsymbol{a}|\boldsymbol{b})$ and $(\boldsymbol{a}'|\boldsymbol{b}')$ is zero iff the inner product (5) of $\phi(\boldsymbol{a}|\boldsymbol{b})$ and $\phi(\boldsymbol{a}'|\boldsymbol{b}')$ is zero. Thus we have

Theorem 4 *Let C be an additive subgroup of $\mathbf{F}_{p^2}^n$ containing p^{n-k} elements, C' its dual with respect to the inner product (5). Suppose that $C' \supseteq C$ and the minimum Hamming weight of $C' \setminus C$ is d. Then any eigenspace of $\phi^{-1}(C)$ is an $[[n, k, d]]_p$ quantum code.*

We next clarify the self-orthogonality of a linear code over $\mathbf{F}_{p^2}$ with respect to (5).

Lemma 5 *Let C be a linear code over $\mathbf{F}_{p^2}$, and C' the dual of C with respect to (5). We define $C^p = \{\boldsymbol{x}^p \mid \boldsymbol{x} \in C\}$ and $(C^p)^\perp$ the dual of C^p with respect to the standard inner product. Then we have $C' = (C^p)^\perp$.*

Proof. It is clear that $C' \supseteq (C^p)^\perp$. Suppose that $\boldsymbol{x} \in C'$. Then for all $\boldsymbol{y}$, $\langle \boldsymbol{x}, \boldsymbol{y}^p \rangle - \langle \boldsymbol{x}, \boldsymbol{y}^p \rangle^p = 0$. Thus $\langle \boldsymbol{x}, \boldsymbol{y}^p \rangle \in \mathbf{F}_p$. Since $\langle \boldsymbol{x}, \omega^p\boldsymbol{y}^p \rangle - \langle \boldsymbol{x}, \omega^p\boldsymbol{y}^p \rangle^p = 0$, $\omega^p \langle \boldsymbol{x}, \boldsymbol{y}^p \rangle \in \mathbf{F}_p$. Since $\omega^p \in \mathbf{F}_{p^2} \setminus \mathbf{F}_p$, we conclude that $\langle \boldsymbol{x}, \boldsymbol{y}^p \rangle = 0$. ∎

Theorem 6 *Let C be an $[n, (n-k)/2]$ linear code over $\mathbf{F}_{p^2}$ such that $C \subseteq (C^p)^\perp$. Suppose that the minimum Hamming weight of $(C^p)^\perp \setminus C$ is d. Then any eigenspace of $\phi^{-1}(C)$ is an $[[n, k, d]]_p$ quantum code.*

3.2 Error correction for p-state systems

In this subsection we consider how to determine the error from measurements with quantum codes obtained via Theorem 6. We retain notations from Theorem 6. Suppose that $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_r$ is an $\mathbf{F}_{p^2}$-basis of C. Then $\mathbf{F}_p$-basis of $\phi^{-1}(C)$ is $(\boldsymbol{a}_1|\boldsymbol{b}_1) = \phi^{-1}(\boldsymbol{g}_1), (\boldsymbol{a}_2|\boldsymbol{b}_2) = \phi^{-1}(\omega\boldsymbol{g}_1), \ldots, (\boldsymbol{a}_{2r}|\boldsymbol{b}_{2r}) = \phi^{-1}(\omega\boldsymbol{g}_r)$. We assume that for $i = 1, \ldots, 2r$ we can perform a measurement M_i whose eigenspaces are exactly the same as those of $X(\boldsymbol{a}_i)Z(\boldsymbol{b}_i)$. Suppose that the error collapsed to E which corresponds to $\phi^{-1}(\boldsymbol{e})$ for some $\boldsymbol{e} \in \mathbf{F}_{p^2}^n$ via $X(\cdot)Z(\cdot)$, and the original quantum state is $|\psi\rangle$. By the measurement M_i, we can know which eigenvalue of $X(\boldsymbol{a}_i)Z(\boldsymbol{b}_i) \quad E|\psi\rangle$ belongs to. By Eq.(2)

$$X(\boldsymbol{a}_i)Z(\boldsymbol{b}_i)E|\psi\rangle = \lambda^{\ell}E|\psi\rangle,$$

where ℓ is the alternating inner product (1) of $(\boldsymbol{a}_i|\boldsymbol{b}_i)$ and $\phi^{-1}(\boldsymbol{e})$, which is denoted by $s_i \in \mathbf{F}_p$. Then we have

$$\begin{aligned} \langle \boldsymbol{g}_i, \boldsymbol{e}^p\rangle - \langle \boldsymbol{g}_i^p, \boldsymbol{e}\rangle &= (\omega^2 - \omega^{2p})s_{2i}, \\ \langle \omega\boldsymbol{g}_i, \boldsymbol{e}^p\rangle - \langle \omega^p\boldsymbol{g}_i^p, \boldsymbol{e}\rangle &= (\omega^2 - \omega^{2p})s_{2i+1}. \end{aligned}$$

It follows that $\langle \boldsymbol{g}_i^p, \boldsymbol{e}\rangle = (\omega^2 - \omega^{2p})(\omega s_{2i} - s_{2i+1})/(\omega^p - \omega)$. $\{\boldsymbol{g}_1^p, \ldots, \boldsymbol{g}_r^p\}$ can be used as rows of the check matrix of $(C^p)^{\perp}$. If we have a classical decoding algorithm for $(C^p)^{\perp}$ finding the error $\boldsymbol{e}$ from a classical syndrome $\langle \boldsymbol{g}_1^p, \boldsymbol{e}\rangle$, $\ldots$, $\langle \boldsymbol{g}_r^p, \boldsymbol{e}\rangle$, then we can find the quantum error E.

4 Construction of quantum codes for p^m-state systems from classical codes

4.1 Codes for p^m-state systems

In this subsection we show a construction of quantum codes for p^m-state systems from classical linear codes over $\mathbf{F}_{p^{2m}}$. Our construction is based on the construction [3] by Chen which constructs quantum codes for 2-state systems from linear codes over $\mathbf{F}_{2^{2m}}$. We modify his construction so that we can estimate the minimum weight (4) from the original code over $\mathbf{F}_{p^{2m}}$.

We fix a normal basis $\{\theta, \theta^p, \ldots, \theta^{p^{2m-1}}\}$ of $\mathbf{F}_{p^{2m}}$ over $\mathbf{F}_p$. There always exists a normal basis of $\mathbf{F}_{p^{2m}}$ over $\mathbf{F}_p$ [7, Section VI,§13]. For $\boldsymbol{a} = (a_1, \ldots, a_m, b_1, \ldots, b_m), \boldsymbol{a}' = (a'_1, \ldots, a'_m, b'_1, \ldots, b'_m) \in \mathbf{F}_p^{2m}$, we define $\phi(\boldsymbol{a}) = a_1\theta + a_2\theta^p + \cdots + a_m\theta^{p^{m-1}} + b_1\theta^{p^m} + \cdots + b_m\theta^{p^{2m-1}}$, and $T(\boldsymbol{a}, \boldsymbol{a}') = c_{m+1} - c_1 \in \mathbf{F}_p$, where $\phi(\boldsymbol{a})\phi(\boldsymbol{a}')^{p^m} = c_1\theta + \cdots + c_{2m}\theta^{p^{2m-1}}$ and $c_i \in \mathbf{F}_p$. Then T is a bilinear form.

Lemma 7 *T is alternating and nondegenerate.*

Proof. First we show that T is alternating, that is, $T(\boldsymbol{a}, \boldsymbol{a}) = 0$ for all $\boldsymbol{a} \in \mathbf{F}_p^{2m}$. Let $x = \phi(\boldsymbol{a}) \in \mathbf{F}_{p^{2m}}$, and $xx^{p^m} = c_1\theta + \cdots + c_{2m}\theta^{p^{2m-1}}$ for $c_i \in \mathbf{F}_p$. Then

$(xx^{p^m})^{p^m} = c_{m+1}\theta + c_{m+2}\theta^p + \cdots + c_{2m}\theta^{p^{m-1}} + c_1\theta^{p^m} + \cdots + c_m\theta^{p^{2m-1}}$. Since $(xx^{p^m})^{p^m} = x^{p^m}x$, $c_i = c_{i+m}$ for $i = 1, \ldots, m$. Hence $T(\boldsymbol{a}, \boldsymbol{a}) = 0$.

Next we show the nondegeneracy. We assume that $x \neq 0$, which implies that $\boldsymbol{a} \neq 0$. Since $x(\theta/x^{p^m})^{p^m} = \theta^{p^m}$, $T(\boldsymbol{a}, \phi^{-1}(\theta/x^{p^m})) = 1$, which shows the nondegeneracy. ∎

Lemma 8 *By abuse of notation, we denote by T the representation matrix of the bilinear form T with respect to the standard basis of $\mathbf{F}_p^{2m}$, that is, for $\boldsymbol{a}, \boldsymbol{b} \in \mathbf{F}_p^{2m}$, we have $T(\boldsymbol{a}, \boldsymbol{b}) = \boldsymbol{a}T\boldsymbol{b}^t$. Let I_{2m} be the $2m \times 2m$ unit matrix and $S = \begin{pmatrix} 0 & I_{2m} \\ -I_{2m} & 0 \end{pmatrix}$. There exists a nonsingular $2m \times 2m$ matrix D such that $DTD^t = S$.*

Proof. See [7, Chapter XV] and use the previous lemma. ∎

For $\boldsymbol{c} = (c_1, \ldots, c_n) \in \mathbf{F}_{p^{2m}}^n$, let $(a_{i,1}, \ldots, a_{i,m}, b_{i,1}, \ldots, b_{i,m}) = \phi^{-1}(c_i)D^{-1} \in \mathbf{F}_p^{2m}$. We define $\Phi(\boldsymbol{c}) = (a_{1,1}, a_{1,2}, \ldots, a_{1,n}, a_{2,1}, \ldots, a_{n,m}, b_{1,1}, \ldots, b_{n,m})$. Then it is clear that the Hamming weight of $\boldsymbol{c}$ is equal to the weight (4) of $\Phi(\boldsymbol{c})$, since D is a nonsingular matrix.

For $\boldsymbol{a}, \boldsymbol{b} \in \mathbf{F}_{p^{2m}}^n$ we consider an inner product

$$\langle \boldsymbol{a}, \boldsymbol{b}^{p^m} \rangle. \tag{6}$$

Proposition 9 *Let $C \subset \mathbf{F}_{p^{2m}}^n$ be a linear code over $\mathbf{F}_{p^{2m}}$, and C' the dual of C with respect to (6). Then the dual of $\Phi(C)$ with respect to (1) is $\Phi(C')$.*

Proof. For $\boldsymbol{e} = (e_1, \ldots, e_n), \boldsymbol{e}' = (e'_1, \ldots, e'_n) \in \mathbf{F}_{p^{2m}}^n$, the inner product (1) of $\Phi(\boldsymbol{e}) = (a_{1,1}, \ldots, a_{n,m}, b_{1,1}, \ldots, b_{n,m})$ and $\Phi(\boldsymbol{e}') = (a'_{1,1}, \ldots, a'_{n,m}, b'_{1,1}, \ldots, b'_{n,m})$ is equal to

$$\begin{aligned} \sum_{i=1}^{n}\sum_{j=1}^{m}(a_{i,j}b'_{i,j} - a'_{i,j}b_{i,j}) &= \sum_{i=1}^{n} \phi^{-1}(e_i)D^{-1}S(D^{-1})^t\phi^{-1}(e'_i)^t \\ &= \sum_{i=1}^{n} T(\phi^{-1}(e_i), \phi^{-1}(e'_i)). \end{aligned}$$

If $e_i e_i'^{p^m} = c_1\theta + \cdots + c_{2m}\theta^{p^{2m-1}}$, then $T(\phi^{-1}(e_i), \phi^{-1}(e'_i)) = c_{m+1} - c_1$. Thus if $\langle \boldsymbol{e}, \boldsymbol{e}'^{p^m} \rangle = 0$ then the inner product (1) of $\Phi(\boldsymbol{e})$ and $\Phi(\boldsymbol{e}')$ is zero, which implies $\Phi(C')$ is contained in the dual of $\Phi(C)$ with respect to (1). Comparing their dimensions as $\mathbf{F}_p$-spaces we see that they are equal. ∎

Theorem 10 *Let $C \subset \mathbf{F}_{p^{2m}}^n$ be an $[n, (n-k)/2m]$ linear code over $\mathbf{F}_{p^{2m}}$, $C^{p^m} = \{\boldsymbol{x}^{p^m} \mid \boldsymbol{x} \in C\}$, and $(C^{p^m})^\perp$ the dual code of C^{p^m} with respect to the standard inner product. Suppose that $C \subseteq (C^{p^m})^\perp$, and the minimum Hamming weight of $(C^{p^m})^\perp \setminus C$ is d. Then the minimum weight (4) of $\Phi(C)$ is d, and $\Phi(C)$ is self-orthogonal with respect to the inner product (1). Any eigenspace of $\Phi(C)$ is an $[[n, k, d]]_{p^m}$ quantum code.*

4.2 Error correction for p^m-state systems

In this subsection we consider how to determine the error from measurements with quantum codes obtained via Theorem 10. We retain notations from Theorem 10. Suppose that $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_r$ is an $\mathbf{F}_{p^{2m}}$-basis of C.

We fix a basis $\{\alpha_1, \ldots, \alpha_{2m}\}$ of $\mathbf{F}_{p^{2m}}$ over $\mathbf{F}_p$. Then $\mathbf{F}_p$-basis of $\Phi(C)$ is $\{\Phi(\alpha_j \boldsymbol{g}_i) \mid i = 1, \ldots, r,\ j = 1, \ldots, 2m\}$. First we shall show how to calculate $\langle \boldsymbol{e}, \boldsymbol{g}_i^{p^m} \rangle$ for each i. For $j = 1, \ldots, 2m$, let $(\boldsymbol{a}_j | \boldsymbol{b}_j) = \Phi(\alpha_j \boldsymbol{g}_i)$. Suppose that the error occurred corresponds to $\Phi(\boldsymbol{e})$ for $\boldsymbol{e} \in \mathbf{F}_{p^{2m}}^n$. As in Section 3.2, by measurements we can know the inner product (1) of $\Phi(\boldsymbol{e})$ and $\Phi(\alpha_j \boldsymbol{g}_i)$, denoted by s_j, for $j = 1, \ldots, 2m$.

For $x = c_1\theta + \cdots + c_{2m}\theta^{p^{2m-1}} \in \mathbf{F}_{p^{2m}}$, $c_1, \ldots, c_{2m} \in \mathbf{F}_p$, we define $P(x) = c_{m+1} - c_1$. Then P is a nonzero $\mathbf{F}_p$-linear map. As discussed in the proof of Proposition 9, $s_j = P(\langle \boldsymbol{e}, \alpha_j^{p^m} \boldsymbol{g}_i^{p^m} \rangle) = P(\alpha_j^{p^m} \langle \boldsymbol{e}, \boldsymbol{g}_i^{p^m} \rangle)$. We define the map $P_{2m} : \mathbf{F}_{p^{2m}} \to \mathbf{F}_p^{2m}$, $x \mapsto (P(\alpha_1^{p^m} x), \ldots, P(\alpha_{2m}^{p^m} x))$. Then P_{2m} is an $\mathbf{F}_p$-linear map, and $P_{2m}(\langle \boldsymbol{e}, \boldsymbol{g}_i^{p^m} \rangle) = (s_1, \ldots, s_{2m})$. If P_{2m} is an isomorphism, then finding $\langle \boldsymbol{e}, \boldsymbol{g}_i^{p^m} \rangle$ from $(s_1, \ldots, s_{2m})$ is a trivial task, merely a matrix multiplication. We shall show that P_{2m} is an isomorphism.

Lemma 11 *[7, Theorem 6.1, Chapter III] Let W be a $2m$-dimensional vector space over a field K with a basis $\{x_1, \ldots, x_{2m}\}$, and $\widehat{W}$ the dual of W, that is, the K-linear space consisting of linear maps from W to K. Then there exists a basis $\{f_1, \ldots, f_{2m}\}$ of $\widehat{W}$ such that $f_k(x_j) = \delta_{jk}$. $\{f_1, \ldots, f_{2m}\}$ is called the* dual basis*.*

Lemma 12 *There exist $\beta_1, \ldots, \beta_{2m} \in \mathbf{F}_{p^{2m}}$ such that $P(\alpha_j^{p^m} \beta_k) = \delta_{jk}$.*

Proof. Notice that $\{\alpha_1^{p^m}, \ldots, \alpha_{2m}^{p^m}\}$ is an $\mathbf{F}_p$-basis of $\mathbf{F}_{p^{2m}}$. The dual space $\widehat{\mathbf{F}}_{p^{2m}}$ can be regarded as $\mathbf{F}_{p^{2m}}$-linear space by defining $xf : u \mapsto f(xu)$ for $x \in \mathbf{F}_{p^{2m}}$ and $f \in \widehat{\mathbf{F}}_{p^{2m}}$. Let $f_1, \ldots, f_{2m}$ be the dual basis of $\{\alpha_1^{p^m}, \ldots, \alpha_{2m}^{p^m}\}$. Since $\widehat{\mathbf{F}}_{p^{2m}}$ is one-dimensional $\mathbf{F}_{p^{2m}}$-linear space and $0 \neq P \in \widehat{\mathbf{F}}_{p^{2m}}$, f_k can be written as $\beta_k P$ for some $\beta_k \in \mathbf{F}_{p^{2m}}$. It is clear that $P(\alpha_j^{p^m} \beta_k) = \delta_{jk}$. ∎

Proposition 13 *P_{2m} is an isomorphism.*

Proof. It is suffice to show that P_{2m} is surjective. For $(a_1, \ldots, a_{2m}) \in \mathbf{F}_p^{2m}$, $P_{2m}(a_1\beta_1 + \cdots + a_{2m}\beta_{2m}) = (a_1, \ldots, a_{2m})$, where β_k is as in the previous lemma. ∎

As in Section 3.2, the error $\boldsymbol{e}$ can be determined by a classical error-correcting algorithm for $(C^{p^m})^\perp$ from $\langle \boldsymbol{g}_1^{p^m}, \boldsymbol{e} \rangle$, $\ldots$, $\langle \boldsymbol{g}_r^{p^m}, \boldsymbol{e} \rangle$.

Acknowledgment

We would like to thank Prof. Hao Chen, Department of Mathematics, Zhongshan University, People's Republic of China, for providing his paper [3]. Without his paper, our paper might not be in the present form.

References

[1] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," Phys. Rev. Lett., vol.78, no.3, pp.405–408, Jan. 1997. LANL eprint quant-ph/9605005.

[2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," IEEE Trans. Inform. Theory, vol.44, no.4, pp.1369–1387, July 1998. LANL eprint quant-ph/9608006.

[3] H. Chen, "Construction of quantum error-correcting codes via algebraic-geometric codes," submitted to IEEE Trans. Inform. Theory, Apr. 1999.

[4] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," Phys. Rev. A, vol.54, no.3, pp.1862–1868, Sept. 1996. LANL eprint quant-ph/9604038.

[5] E. Knill, "Non-binary unitary error bases and quantum codes," LANL eprint quant-ph/9608048, Aug. 1996.

[6] E. Knill, "Group representations, error bases and quantum codes," LANL eprint quant-ph/9608048, Aug. 1996.

[7] S. Lang, Algebra, third ed., Addison-Wesley, 1993.

[8] E. M. Rains, "Nonbinary quantum codes," LANL eprint quant-ph/9703048, Mar. 1997.